IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
v.	**:**	**CRIM. NO. 24-MJ-1338**
RUBEN FILIPE GABRIEL MARTINS a/k/a FEEPSY	**:**	

GOVERNMENT'S MOTION FOR PRETRIAL DETENTION

The United States of America, by and through Jacqueline C. Romero, United States Attorney for the Eastern District of Pennsylvania, and Anthony J. Carissimi, Danielle Bateman, and Sarah Wolfe Assistant United States Attorneys for the District, hereby moves this Honorable Court to detain the defendant prior to trial.

I. FACTS AND EVIDENCE

The defendant stole more than $60,000 in cryptocurrency on behalf of an enterprise known as "The Com." As explained in more depth below, the Com consists of a geographically diverse group of individuals, organized in various subgroups, all of whom engage in various types of criminal activity to include corporate intrusions, SIM swapping, cryptocurrency theft, commissioning in real life violence, and swatting. With respect to this defendant, investigators have uncovered evidence showing that he has engaged in an ongoing scheme to steal cryptocurrency that has netted him thousands of dollars. As part of his participation in the enterprise, the defendant is now charged with stealing approximately $60,000 worth of cryptocurrency from a victim who resides in the Eastern District of Pennsylvania.

a) Background on "The Com"

The Com operates as a widespread criminal conspiracy. The object of the conspiracy is to gain access to protected financial systems through cyber hacking to steal or extort funds. The targeted funds are often held as cryptocurrency. Much like more traditional organized crime groups, members of the Com protect and promote themselves through intimidation, terror, and violence. The group's cyber intrusions include corporate intrusions, malware development and deployment, and individual account compromises. The main goal of these intrusions is to obtain personal information—e-mail addresses, passwords, physical addresses, and phone numbers—which can then be used to steal money or cryptocurrency.

Membership within the Com is predicated upon a willingness to engage in criminal activity and an ability to assist members in their criminal endeavors. Within The Com, various subgroups exist, organized in hierarchical structures. The subgroups and individuals within the subgroups coordinate with each other and work collaboratively to maximize profits from their crimes. Members of the Com also engage in intrusions into telecommunications companies and other companies to support and facilitate SIM swapping. While the SIM swapping and intrusions seem to be the primary ways Com members monetize their criminal activity, its members also engage in various other cybercrimes, including phishing schemes, and "in real life" crimes of violence and harassment. As a whole, the group is responsible for tens of millions of dollars in stolen funds.

b) The Instant Offense Conduct

On April 6, 2024, a resident of the Eastern District of Pennsylvania ("Victim 1") reported to a local Police Department that $60,682.57 in cryptocurrency had been stolen from his Coinbase account. Victim 1 advised that on April 5, 2024, in the late evening hours, he received a text message purportedly from Yahoo, stating that a phone number change had been made on his Yahoo e-mail account and to reply with "N" if it was unauthorized. Victim 1 responded, "N" to the text message.

Shortly thereafter, on April 6, 2024, Victim 1 received a call in which the caller claimed he was a representative from Coinbase. The caller advised Victim 1 that his Coinbase account had been compromised. Victim 1 was instructed to provide his Two Factor Authentication (2FA) code from Coinbase to facilitate a transfer to a secure wallet.[1] During the call, Victim 1 also received a text message from 818-850-2627 (the "2627 Number") that provided a link to a website, "191284-Coinbase.com." Victim 1 could not recall whether he clicked on the link or entered his login credentials. Believing the caller was from Coinbase, Victim 1 provided the 2FA codes as instructed. Victim 1 subsequently realized this was a scam and that his Coinbase account had been drained. At the time of the theft, Victim 1's funds were valued at $60,682.57.

Criminal actors engaged in phishing offenses frequently register domains closely resembling the branding and layout of the authentic domain. The use of a hyphen creates a unique domain not affiliated with the actual brand. Victims of phishing offenses frequently mistake this for a subdomain, which is frequently used by brands for various functions, including securing

[1] Coinbase offers a security setting whereby Coinbase sends a 2FA challenge before authorizing a fund transfer. A user must enter a code that he receives by text message in order to complete a transaction.

accounts. Here, the "191284-Coinbase.com" phishing domain was registered to a user in Switzerland. The registration name was also connected to 214 other similar domains.

Cryptocurrency blockchain tracing showed that Victim 1's stolen funds were subsequently transferred to several cryptocurrency exchange accounts, with the majority of funds being transferred through smart contracts and cryptocurrency mixing services. Additional analysis revealed a portion of the stolen funds were deposited into a gambling website account that the defendant had previously funded on 27 separate occasions. Members of the Com frequently use gambling websites to launder stolen funds. Records from the gambling website revealed that the defendant provided the email address feepsy@riseup.net and an Italian Passport with a different name during account registration.

Investigators served legal process on the -2627 Number which sent the Coinbase phishing domain to Victim 1. The records showed that between April 5 and May 3, 2024, the 2627 Number sent or received text messages to/from 23 unique phone numbers. Approximately 18 of the text messages contained phishing links or outgoing messages which appear to involve phishing attempts. The -2627 number was registered using an e-mail address that was connected by cookies to other e-mail accounts bearing the names "filipemartins20111" and "feepsbruh." Both of these are variations on the defendant's name. Another Google voice number used by the defendant to target the victim also sent threats to other likely victims, including telling one likely victim "Thanks for the NFTS and the 150 thousand XYO" and "youll never know who we are but we know everything about you." To another likely victim, the Google voice number used by the Defendant sent what appears to be the victim's home address and writing "dead in a week."

The -2627 number also communicated with a company that services Bitcoin ATMs. The communications included text messages reporting a problem with one of the company's machines. A review of the responsive records revealed the defendant's Portugal citizen identification card and surveillance images of the defendant at the ATM. In addition, the defendant used another individual's personal identifying information, without authorization, in order to satisfy some of the know-your-customer requirements for accessing the Bitcoin ATM.

In sum, the evidence shows the defendant sent dozens of phishing messages with links to fake Coinbase websites that were used to steal tens of thousands of dollars in cryptocurrency. He committed these crimes in furtherance of an ongoing criminal conspiracy involving sophisticated cybercriminals.

II. DEFENDANT INFORMATION

The defendant, a 23-year-old male, is not a citizen of the United States. He was born in Portugal and currently resides in Scottland. He does not have any known ties to the Eastern District of Pennsylvania or the United States in general. He travels between Scotland and the United States only occasionally, and upon arrival in the United States provided a home address in the United Kingdom which appears to be a mail delivery service. While committing these crimes, the defendant utilized a fake Italian passport and the identity of another individual living in Texas to circumvent legal "know your customer" requirements. The defendant claims to be self-employed at a marketing firm, but that information remains unverified. The government's investigation suggests his only source of income is illegal criminal activity.

III. MAXIMUM PENALTIES

The maximum penalty for wire fraud, in violation of 18 U.S.C. § 1343, is twenty years' imprisonment, a $250,000 fine, and a $100 special assessment. 18 U.S.C. § 1343.

IV. ARGUMENT

The defendant should be detained pending trial. Courts considering detention must weigh several factors to determine whether there are conditions of release that will both reasonably assure the appearance of the defendant and will assure the safety of the community. First, the court must examine the "nature and circumstances of the offense charged, including whether the offense is crime of violence." *Id.* § 3142(g)(1). Second, it must look at the "weight of the evidence against the person." *Id.* § 3142(g)(2). Third, it must examine the history and characteristics of the defendant. *Id.* § 3142(g)(3). Finally, it must weigh "the nature and seriousness of the danger to any person or the community that would be posed by the person's release." *Id.* § 3142(g)(4). The balance of these factors weigh in favor of detention.

First, the nature and circumstances of the offense charged weigh in favor of the detention. Although wire fraud itself is not inherently dangerous or necessarily indicative of a defendant who presents a flight risk, the particular circumstances of this offense warrant detention for at least two reasons. First, the defendant committed this crime as part of a large-scale cybercriminal group that is prone to violence—include bricking attacks, swatting calls, and in-real-life violence. The defendant's access to vast sums of cryptocurrency and his ability to contract with a network of criminals willing to seek retribution presents a unique danger to both the victim of the offense and potential witnesses. Second, the defendant committed this crime using at least two means of false identification—an Italian passport and the identity of a man in Texas. If released,

the defendant will be in a district with which he has no connection and will be able to abscond by accessing fraudulent identification documents. This will make compelling his appearance at trial impossible. The first factor therefore weighs in favor of detention.

Next, the Court must examine the weight of the evidence against the defendant. As stated above, the evidence in this case is strong. The government has amassed overwhelming digital evidence—including pictures of the defendant using a Bitcoin ATM to access ill-gotten gains—to show that the defendant was at the center of a phishing conspiracy. The near certainty of conviction in this case provides a powerful incentive for the defendant to flee. The second factor therefore also weighs in favor of detention.

The history and characteristics of the defendant also weigh heavily in favor of detention. In short, the defendant has nowhere to go. He has no residence in the Eastern District of Pennsylvania or the United States. His identification documents, wallet, phone, and cryptocurrency wallet were seized as evidence. Without a stable residence, the defendant cannot be effectively monitored. Moreover, members of the Com regularly communicate using online social media and other encrypted messaging platforms that are difficult for law enforcement to track and accessible by cell phone, computers, and tablet. Pretrial Services (PTS) officers are (1) limited to inspection of items that are in plain view of the officers, and (2) not permitted to seize electronic evidence. Thus, the PTS officers can only "search" for items which have been left out in the open by the defendant. Even if they were to find such evidence, PTS officers are not permitted to seize electronics—even those electronics which would be prohibited by a Court order, such as an unregistered smart phone or computer.

Even if the defendant were to be released into a halfway house, that is no guarantee that he would be prevented from committing crimes. In fact, a known coconspirator of the defendant has been charged in this district for orchestrating a campaign of bomb threats against a juvenile *while he was in a California halfway house awaiting trial.* That same individual has previously traveled together on lavish vacations with the defendant spending stolen cryptocurrency. No conditions of release can prevent the defendant from accessing the platforms that he previously used to commit crimes, thereby rendering any computer restrictions completely unenforceable. He should be detained pending trial.

V. CONCLUSION

For these reasons, no condition or combination of conditions will reasonably assure the safety of the community and the defendant's appearance at trial. WHEREFORE, the government respectfully requests the Court to detain this defendant prior to trial.

Respectfully submitted,

JACQUELINE C. ROMERO
United States Attorney

/s/ *Anthony J. Carissimi*
ANTHONY J. CARISSIMI
Assistant United States Attorney
DANIELLE BATEMAN
Assistant United States Attorney
SARAH WOLFE
Assistant United States Attorney

CERTIFICATE OF SERVICE

I certify that a copy of the Government's Motion for Pretrial Detention was served by e-filing and email on the following defense counsel:

Lawrence Bozzelli
Attorney for Ruben Filipe Gabriel Martins

/s/ *Anthony J. Carissimi*
ANTHONY J. CARISSIMI
Assistant United States Attorney

Date: September 24, 2024